DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG

22 March 2007

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy # 12: System Security Life Cycle

1. References:

a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

b. AR 380-5, Department of the Army Information Security Program, 29 September 2000.

c. AR 25-2, Information Systems Security, 14 November 2003.

d. AR 380-67, Personnel Security Program, 9 September 1988.

e. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

f. DOD Instruction 8500.2, “Information Assurance (IA) Implementation”, 6 February 2003.

g. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation (C&A) Process, 30 December 1997.

h. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000.

i. DoD CIO Guidance and Policy Memorandum No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000.

j. ISS Policy Change Message (6R00024515U.CGS), From: DA Washington // SAIS-IAS, re: New IA Personnel Structure, Interim Policy, 23 June 2000.

2. Purpose of Policy: The 4ID G6 IA personnel are responsible for providing AIS security to safeguard information systems owned by 4ID organizations. The purpose of these safeguards is to prevent unauthorized access, modification, deletion, or denial of service to information and system resources. As technology matures and evolves, system security and information assurance technology needs to evolve simultaneously. This policy defines a system security life cycle for the 4ID that ensures system security measures stay current with evolving technology.

3. Applicability: This policy applies to all soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to 4ID networks.

4. Responsibilities:

a. Commanders, directors, and supervisors at all levels will ensure that subordinate personnel cooperate in the development, maintenance, and awareness of 4ID IA security policies and procedures.

b. The Directors of 4ID service providers, and the Information Assurance Manager (IAM) shall be responsible for developing and maintaining information security practices and procedures consistent with relevant U.S. Army and 4ID policies.

5. Policy:

a. The System Security Life Cycle for 4ID shall be defined in four levels consistent with the Federal Information Systems Control Audit Manual, Information Security Maturity Framework. Level 1 is aligned with guidance in the FISCAM (Federal Information Systems Control Audit Manual developed by GAO). Levels 2-4 were developed by the Security, Privacy, and Critical Infrastructure Committee of the Federal CIO Council for the purpose of illustrating the concepts envisioned for the higher levels in the maturity framework.

b. Level 1, as defined in Table 1, is detailed in this document because of the confidence in the objectives identified in this level as well as the extent to which relevant policies have been developed within the U.S. Army and the 4ID.

c. Levels 2 through 4 of the maturity framework are refined as the process matures. In general, these levels reflect progression to the use of effective tools and methods in Level 2; endowment of a coordinated and integrated set of protection measures in Level 3; and efficient implementation and use of automated enforcement in Level 4. Several policies have been developed within the 4ID that address a number of concepts identified in the higher levels.

Table 1:

Level 1	• Security Management And Framework Processes ○ Periodically Assess Risks *(4ID Policy)* ○ Document An Entity-Wide Security Program Plan *(AR25-1, AR 380-19, 4ID G6 Policies)* ○ Establish A Security Management Structure And Clearly Assign Security Responsibilities *(AR 380-19, ISS Policy Change message dated 23 June 2000 re: New IA Personnel Structure)* ○ Implement Effective Security-Related Personnel Policies *(AR 380-67)* ○ Monitor The Security Program's Effectiveness And Make Changes As Needed *(4ID G6 Policies)*
Level 2 *(4ID Policies)*	• Foundation Protection ○ Boundary/perimeter protection ○ Intrusion detection and reporting ○ Virus protection ○ Password policy ○ Security-related personnel policies/training
Level 3 *(4ID Policies)*	• Integrated Security Management ○ Security architecture ○ Incident response capability ○ Patches distribution
Level 4	• Managed Security Protection Capability ○ Certified system administrators ○ Automated patch update

d. Control Techniques and Suggested Audit Procedures for Critical Elements in Level 1.

Periodically Assess Risks	
Control Activity	**Control Techniques**
Risks are Periodically Assessed. (ref. 4ID Policy on Continuity	Independent risk assessments are performed and documented on a regular basis or whenever systems, facilities, or other conditions change. Risk assessments should be performed once a year initially, until reliable controls

of Operations Plans)	are in place and the system architecture has matured and stabilized. Thereafter, risk assessments may be performed as required for DITSCAP. The risk assessment considers data sensitivity and integrity and the range of risks to the entity's systems and data. Final risk determinations and related management approvals are documented and maintained on file. (Such determination may be incorporated in the security program plan, which is discussed in the next section).

Document An Entity-Wide Security Program Plan

Control Activity	Control Techniques
A Security plan is documented and approved. (ref. AR380-19, AR 25-1, 4ID G6 Policies)	A security program plan has been documented that: • Covers all major facilities and operations • Has been approved by key affected parties, and • Covers the topics prescribed by OMB Circular A-130 (general support systems/major applications) • Rules of the system/Application rules • Training/Specialized training • Personnel controls/Personnel security • Incident response capability • Continuity of support/Contingency planning • Technical security/Technical controls • System interconnection/Information Sharing • Public access controls
The plan is kept current.	The plan is reviewed periodically and adjusted to reflect current conditions and risks.

Establish A Security Management Structure And Clearly Assign Security Responsibilities

Control Activity	Control Techniques
A security management structure has been established. (ISS Policy Change, AR380-19, 4ID G6 Policies)	The security program plan establishes a security management structure with adequate independence, authority, and expertise. An information systems security manager has been appointed at an overall level and at appropriate subordinate levels.
Information security responsibilities are clearly assigned. (ISS Policy Change, AR380-19, 4ID G6 Policies)	The security plan clearly identifies who owns computer-related resources and who is responsible for managing access to computer resources. Security responsibilities and expected behaviors are clearly defined for (1) information resources owners and users, (2) information resources management and data processing personnel, (3) senior management, and (4) Information Assurance and security administrators.
Owners and users are aware of security policies. (4ID G6 Policies)	An ongoing security awareness program has been implemented. It includes first-time training for all new employees, contractors, and users, and periodic refresher training thereafter. Security policies are distributed to all affected personnel, including system/application rules and expected behaviors.

Implement Effective Security-Related Personnel Policies

Control Activity	Control Techniques
Hiring, transfer, termination, and performance policies address security. (AR380-67)	For prospective employees, references are contacted and background checks performed. Periodic reinvestigations are performed at least once every 5 years, consistent with the sensitivity of the position per criteria from the Office of Personnel Management. Confidentiality or security agreements are required for employees and contractors assigned to work with confidential information. Regularly scheduled vacations exceeding several days are required, and the individual's work is temporarily reassigned. Regular job or shift rotations are required. Termination and transfer procedures include: • Exit interview procedures; • Return of property, keys, identification cards, passes, etc.; • Notification to security management of terminations and prompt revocation of Ids and passwords; • Immediately escorting terminated employees out of the entity's facilities; and • Identifying the period during which nondisclosure requirements remain in effect.
Employees have adequate training and expertise. (AR380-5, 4ID G6 Policies)	Skill needs are accurately identified and included in job descriptions, and employees meet these requirements. A training program has been developed. Employee training and professional development are documented and monitored.

Monitor The Security Program's Effectiveness And Make Changes As Needed

Control Activity	Control Techniques
Management periodically assesses the appropriations of security policies and compliance with them. (DODI 5200.40 - DITSCAP, 4ID G6 Policies)	The entity's IS security program is subjected to periodic reviews. Major applications undergo independent review or audit at least every 3 years. Major systems and applications are authorized or accredited by the managers' whose missions they support Top management initiates prompt action to correct deficiencies.
Management ensures that corrective actions are efficiently implemented. (4ID G6 Policies)	Corrective actions are tested after they have been implemented and monitored on a continuing basis.

6. The IAM shall chair a committee comprised of the 4ID Information Assurance Network Manager (IANM), and selected Information Assurance Network Manager/Officer (IANM/Os), and other

appointees as deemed appropriate, that review 4ID security measures and makes recommendations for improving the effectiveness of security policies and procedures. Risk Assessments, system scans, and Remedy help desk trouble tickets completed within the previous year, among other sources of information, shall be used as sources of information during the review process. The annual report shall include a summary of significant IA security accomplishments and incidents. The annual report shall be submitted to the 4ID that addresses the adequacy of 4ID IA security measures and presents cost-effective alternatives to reduce risks. The Annual Report of 4ID IA Security shall be submitted no later than 30 June each year.

7. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding